Exercises lecture 2/JL Roch - Complexity

Exercise 1. Merkle-Hellman Consider Merkle-Hellman protocol (MH). Bob chooses a super-increasing secret sequence of $n = 1000$ integers a_i for $0 \leq i < n$. Alice signs a binary plain text P (a block), computes $C = E_{Bob}(P)$ and sends C to Bob.

1. What is the size of a P ?
2. Give an algorithm that Bob uses to build its secret integers a_i.
3. Deduce that, if $a_0 = c$, we may consider $a_i \leq 4^i.c$.
4. What is the order of the size of the cipher text C ?
5. Write the algorithms for encoding and decoding and analyze their costs.
6. Conclude on the provable security of DH$(b_0, \ldots, b_{n-1}, m)$.

Exercise 2. Primes, big factor and factorization Consider the following decision problems *IS-COMPOSED* and *IS-PRIME.*

IS-COMPOSED :
- Input : a positive integer n ;
- Output : YES iff $\exists 2 \leq a, b < n : n = a \times b$.

IS-PRIME :
- Input : a positive integer n ;
- Output : YES iff n is prime.

1. Prove that IS-COMPOSED $\leq_P$ IS-PRIME and that IS-COMPOSED $\geq_P$ IS-PRIME.
2. Prove that IS-COMPOSED $\in NP$.
3. To what complexity class belongs IS-PRIME ? You have to give a proof of your answer.
4. Indeed, in 2002 Agrawal, Kayal and Saxena provided a deterministic algorithm that computes IS-PRIME(n) in time $\tilde{O}(\log^6 n)$. From this algorithm, what are the complexity classes of IS-PRIME and IS-COMPOSED ?
5. We consider the following decision problem HAS-BIG-FACTOR :

   - Input : two positive integers n and m ;
   - Output : YES iff n has a prime factor larger than m.

   Prove that HAS-BIG-FACTOR$\in$ NP $\cap$ co-NP, i.e. is both in NP and co-NP.
6. The FACTORIZATION problem takes in input an integer n and returns the list of prime factors of n. Prove that FACTORISATION $\leq_P$ HAS-BIG-FACTOR.
   Is there a link between the question "P= ? NP$\cap$co-NP" and the provable security of RSA ?

Exercise 3. RSA Provable security ; Factorization of n from d Consider a RSA system (n, e, d). Let s and t be two integers such that $ed - 1 = t2^s$.

1. Propose a randomized algorithm, based on a variant of Miller-Rabin primality test, that takes in input n, e, d and return the factorization $n = pq$. (Making only one random choice of an element, the algorithm will return either both factors p and q of n, or a failure message.
2. What is the average number of calls required to factorize n ?
3. Conclude on the provable security of the RSA secret key d.

Exercise 4. Discrete Log and highest significant bit Let $(G, \times)$ be a cyclic group of order n generated by $g : G = \{g^i, 0 \leq i \leq n-1\}$.
Consider the following problems :

- **LOG**$_G$:
  - Input : $x \in G$;
  - Output : $i \in= \{0, \ldots, n-1\}$ such that $g^i = x$.
- **PLOG**$_G$:
  - Input : $x \in G$ and an integer t, $0 \leq t < n$.
  - Output : YES iff LOG$_G(x) \geq t$.

Questions :

1. Prove that $\mathrm{PLOG}_G \in NP \cap co - NP$.
2. Prove :
   (a) $\mathrm{PLOG}_G <_P \mathrm{LOG}_G$,
   i.e. if there exists a polynomial-time deterministic algorithm for LOG_G, then there exists a polynomial-time deterministic algorithm for PLOG_G.
   (b) $\mathrm{LOG}_G <_P \mathrm{PLOG}_G$,
   i.e. if there exists a polynomial-time deterministic algorithm for PLOG_G, then there exists a polynomial-time deterministic algorithm for LOG_G.

   Conclude that PLOG_G and LOG_G are *polynomially equivalent*, i.e. there exists a polynomial-time algorithm for one problem iff there exists a polynomial-time algorithm for the other one.
3. Consider the two decision problems PLOG-LSB$_G$ and PLOG-HSB$_G$ that take both in input $x \in G$ and that compute respectively the least and highest significant bit of $\mathrm{LOG}_G(x)$:
   – PLOG-LSB$_G(x)$=YES iff $\mathrm{LOG}_G(x) \equiv 1 \pmod 2$; (least significant bit).
   – PLOG-HSB$_G(x)$=YES iff $\log_2 \mathrm{LOG}_G(x) \geq \left\lfloor \log_2 \frac{p-1}{2} \right\rfloor$; (highest significant bit).
   Compare the complexities of PLOG-LSB$_G$, PLOG-HSB$_G(x)$ and PLOG_G. What do you thing of a cryptographic protocol which security is based on the PLOG-LSB$_G$?

Exercise 5. El Gamal protocol. Let G a cyclic group of order $p-1$ generated by α. Let d be an integer, and $\beta = \alpha^d$. In the following asymmetric protocol (El Gamal), α and β are public while d is kept secret and known only by Bob.
The encoding function encodes x using a random integer k which is kept secret by the encoder. It is given by :

$$\begin{array}{lcl} E_{\alpha,\beta} : G & \rightarrow & G \times G \\ x & \mapsto & (\alpha^k, x.\beta^k) \end{array}$$

1. Bob receives a message (y_1, y_2). How will he decode it ?
2. Prove that a required condition for the protocol to be a one-way trap-door function is that the discrete logarithm is computationally impossible.

Exercise 6. Asymmetric decryption is in NP Consider an asymmetric crypto-system : the public encryption method is denoted E ; the private decryption method is D. For any plain text p, the size of the corresponding cipher text $c = E(p)$ verifies : $|p| \leq |c| \leq |p| + O(1)$.
It is assumed that E is computed in deterministic polynomial (in practice almost linear) time.
Let "COMPUTE-D" be the following problem (note it is not a decision problem) :
– input : an arbitrary cipher text c ;
– output : the plain text $p = D(c)$.

1. Prove that "COMPUTE-D" can be solved in non-deterministic polynomial time.
2. Formulate decision problems related to "COMPUTE-D".
3. How would you preferably choose "D" (w.r.t. previous questions) ?

Exercise 7. Non-deterministic algorithm and certification algorithm We consider
– NP_{NonDet} : the set of decision problems that can be solved by a non-deterministic algorithm in polynomial time.
– NP_{Certif} : the set of decision problems which output YES can be proved (or certified) by a deterministic algorithm in polynomial time.
Prove that $NP_{NonDet} = NP_{Certif}$.

Additional exercises. see CLRS, 2nd edition, Chap 34, NP-Completeness :
– 34.2-5 : Prove that any decision problem in NP can be computed by an algorithm running in time $2^{O(n^k)}$ where n is the size of the input.
– 34.2-9 : Prove that $P \subset NP$ and $P \subset co - NP$.
– 34.2-10 Prove that if $P \neq co - NP$, then $P \neq NP$ *(Hint : contradiction proof)*.
– Prove that $NP =_{P-Cook} co - NP$. Do we have $NP =_{P-Karp} co - NP$?